Table of Contents

NOTE: Due to firmware upgrades, the information in this Instruction Guide may not be identical to what you see on your screen. Check www.startech.com for firmware upgrades or contact us if you encounter any difficulties. (June 2, 2003)

Introduction

Thank you for purchasing a StarTech.com Virtual Presence stand-alone unit, a KVM over IP solution that gives you full web-based remote KVM control over IP, letting you manage your servers from anywhere in the world. The SV1105IPEXT is one of the smallest KVM over IP controls in the world and works across most hardware, OS, or processor platforms. Ideal for ISPs, ASPs, and data centers where downtime must be minimized, this powerful server administration tool allows BIOS-level remote control of target servers and offers standard 128-bit SSL encryption. The SV1105IPEXT allows you to control, reset, and reboot your entire data center from a remote location and is compatible with most KVM switches.

Features

- Allows you to have full keyboard and mouse control - as if you are on location
- Allows server(s) to be controlled from any Web browser which eliminates licensing costs
- Provides excellent remote video quality and industry-leading performance through advanced video detection algorithms
- Patented Mouse-Lok ™ mouse tracking technology auto-corrects remote mouse synchronization errors without user intervention
- Provides a secure remote connection through 128-bit SSL encryption
- Flash upgrade capability
- Uses minimal bandwidth - usable over a 56k dial-up connection
- Extremely compact size - one of the smallest IP based KVMs on the market

Before You Begin

To ensure a quick and easy console installation, please read through this section carefully before attempting to install the device.

Contents

This package should contain:

- 1 x SV1105IPEXT
- 1 x keyboard/mouse cable
- 1 x 12V DC 500mA power adapter

System Requirements

Managed Host Computer:

- Video adapter is non-interlaced and is set to a supported resolution and refresh rate (Quality is maximized at 1024x768@75Hz)
- Mouse acceleration is turned off (See "Mouse Acceleration" below)
- Windows XP/2000/Me/98/NT 4.x, Red Hat Linux 8.0, Novel NetWare v6.0, Mac OS 10.2

Remote Client Computer

- Windows XP/2000/98SE/NT 4.x
- Internet Explorer 5.5 or higher
- 500 Mhz Intel Pentium III processor, 128 Mb RAM (1Gb recommended), 20 Mb free local hard drive space

NOTE: Throughout this manual "managed host" or "host computer" refers to the computer connected to the SV1105IPEXT. "Remote client" or "client computer" refers to the PCs used to access the host computer.

Mouse Acceleration

The managed host computer must have mouse acceleration turned off to use the SV1105IPEXT.

Windows XP

1. From the Control Panel, choose "Printers and Other Hardware."
2. Click on "Mouse."
3. From Mouse Properties, choose "Pointer Options."
4. Make sure that the Motion pointer speed slider bar is centered and deselect "Enhance Pointer Precision."

Windows 2000

1. From the Control Panel, click on "Mouse."
2. From Mouse Properties, click on the Motion tab.
3. Make sure that the Speed slider bar is centered and Acceleration is set to None.

Windows Me/98/NT 4.x

1. From the Control Panel, click on "Mouse."
2. From Mouse Properties, click on the Motion tab.
3. Verify that the Pointer speed bar is to the left.

Linux

1. Execute one of the following command line parameters:

```
xset 0 255
```

or

```
xset m 0
```

NetWare 6.0 servers running Java 1.4.1

1. From the NetWare 6 GUI Environment tool Input tab, select "Turn off mouse acceleration."
2. Click Apply and restart the GUI.

NetWare 6.0 servers running Java 1.3.1 CSP8 or CSP9

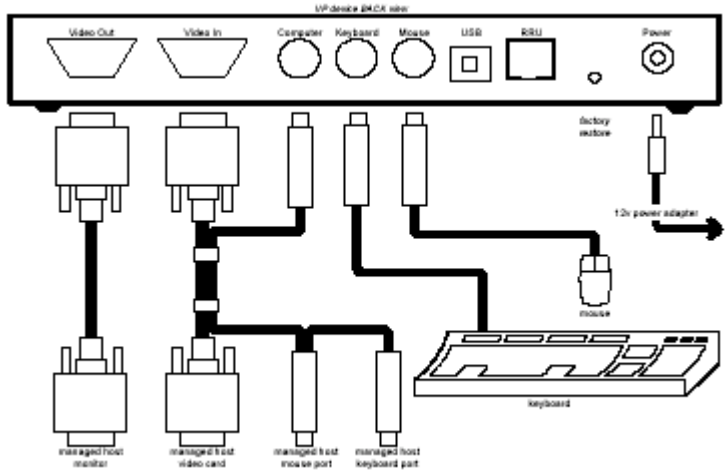
1. Add the following command to the NetWare 6 sys:/java/nwgfx/xinitrc file:

```
xset m 1
```

Installation

This section will guide you through the installation of your SV1105IPEXT. Please read through this section carefully and complete each step in the order listed.

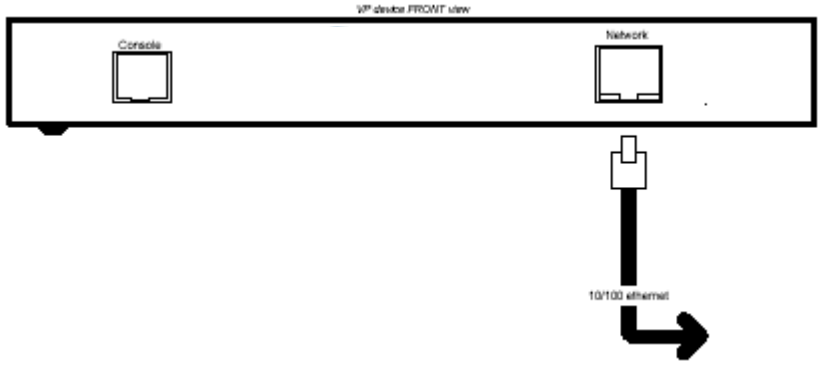
Connecting the Device



1. Connect your keyboard, mouse, and monitor to the **Keyboard, Mouse** and **Video Out** ports on the unit.

NOTE: The **USB** port on the device can be used to connect a USB mouse and keyboard, when available. See Appendix D on page 19 for details.

2. Using the provided cable, connect the purple PS/2 keyboard, PS/2 green mouse, and blue HD-DB15 video connectors into their respective ports on your PC. Plug the black HD-DB15 video and black PS/2 connector into the **Video In** and **Computer** ports on the device.



3. Using a 10/100 Ethernet cable, connect the console to your network using the **Network** port on the front of the device.

4. Plug the 12V DC 500mA power adapter into the **Power** port on the back of the device and plug the other end into an available grounded power source.

Initial Setup

There are two options for setting the device's IP address: using the static IP address or using ARP to set the IP address.

Using the Static IP Address
The device boots to the following defaults:

IP Address:	192.168.1.254
Gateway:	192.168.1.1
Netmask:	255.255.255.0

You can use the device on a subnet that matches the default static IP address or use the Soronti Web Server Device Configuration web page to change the IP address.

–OR–

Using ARP to set the IP Address
ARP is a command line utility available in most OS platforms.

1. Contact your network administrator and obtain a unique IP address.

   IP Address: _____

2. From a client computer attached to the same subnet as the device, open a DOS window and type the following command:

   ```
   arp –s <IP address> <MAC address>
   ```

where `<IP address>` is the IP address obtained from your network administrator (for example, 192.168.1.254) and `<MAC address>` is the 12-digit MAC address listed on the device (for example, FF-FF-FF-FF-FF-FF).

3. Ping the device using the following command:

   ```
   ping <IP address>
   ```

where `<IP address>` is the IP address obtained from your network administrator.

NOTE: While the ping command verifies the IP address, it may return a few "Host not responding" messages. If this message appears four times, however, either you have entered the MAC address incorrectly or the IP address is incorrect.

4. If the ping command was successful, remove the IP address from the ARP table by using the following command:

   ```
   arp –d <IP Address>
   ```

Accessing the Device Through a Firewall

If you are accessing the device through a firewall, make sure that the following Internet ports are available and configured for TCP traffic or packets:

Application/ Services	**Ports (decimal)**
VP Viewer	5900
Update.exe	12296
HTTP	80
SSL	443
Telnet	23
FTP	21

Completing the Setup Process

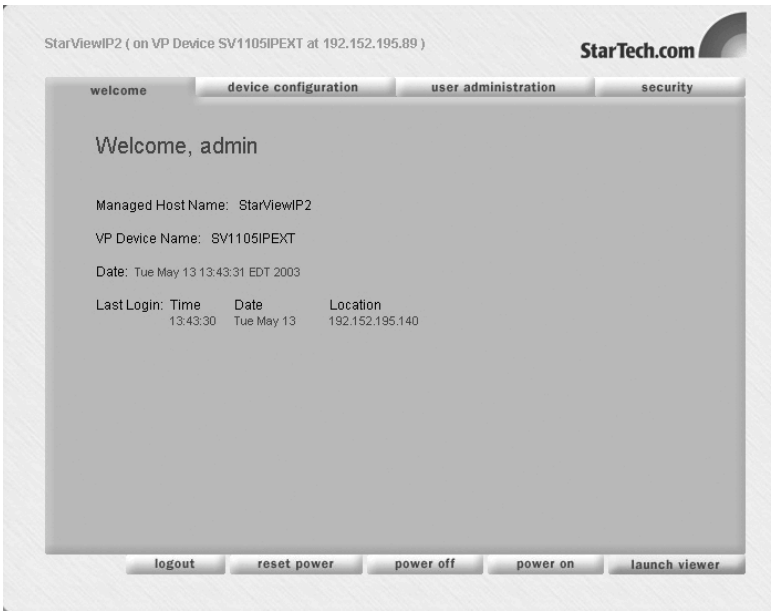
Using the device's web server, you can communicate directly with your device to finalize your initial setup.

Launching the Web Server

1. From a client computer, launch your web browser.
2. Enter the IP address in your address bar and press Enter.
3. On the password screen, enter the following defaults and click **OK**:
   User name: *admin*
   Password: *password*

Using Your Device

You can use the tabs on the top of the screen to navigate through the different device options and configuration screens.



Welcome: Clicking on this tab returns you to the welcome screen shown above.

Device Configuration (pg. 8): The tab lets you set the device's time/date, edit the host name and device name, change the IP address and verify the firmware version and MAC Address.

User Administration (pg. 9): The User Administration page lets you add and manage users assigned to access the device.

Security (pg. 10): The security page allows you to specify different levels of encryption, which can boost device performance or increase the level of security. From the security page, you can also view your security logs (pg. 11).

Logout: Clicking here will log you off the device.

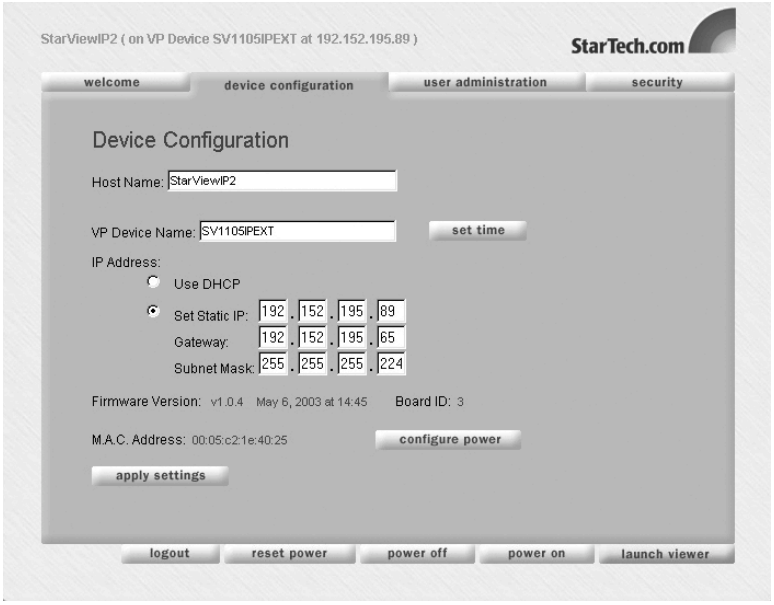
Reset Power/Power Off/Power On: See Appendix B: Connecting a Remote Reboot Unit.

Launch Viewer (pg. 12): Clicking the Launch Viewer button (highlighted in yellow) will allow you to view and control the managed host computer.

Device Configuration

The Device Configuration tab allows you to perform a variety of configuration functions. From here you can change the date/time, change the IP address, and check the device's firmware version and MAC address.

NOTE: To perform functions on the Device Configuration menu, you must be logged in as *admin* or as a user with administrator rights. For more information on assigning administrator privileges, see "User Administration" on page 9.



Setting the Date and Time
Click on **Set Time** and enter the new time and date. Click **Apply Settings**.

Changing the Host Name or Device Name
To change the host or device name, click in the Host Name or VP Device Name fields and enter a new name. When you are finished, click the **Apply Settings** button near the bottom left of the screen.

Changing the static IP address, gateway, or subnet mask
To manually change these settings, click in the fields and enter the new information. When you are finished, click the **Apply Settings** button near the bottom left of the screen.

When applicable, you can receive this information from your DHCP server. For this procedure to work, you must have DHCP services available on the local subnet where the device is installed. Click the **Use DHCP** button to automatically receive this information.

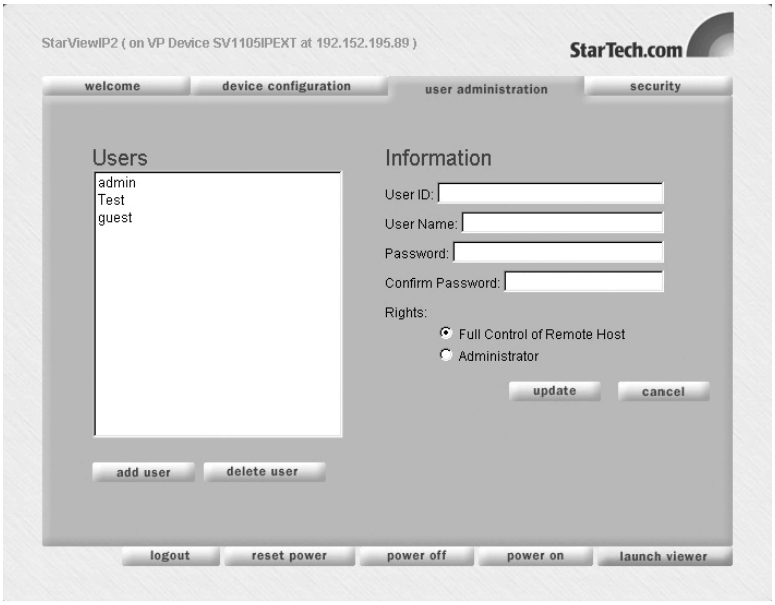
NOTE: If switching between using the DHCP server and setting the information manually, please turn off DHCP, then click **Apply Settings**, then change the information.

Configure Power: For information on the remote reboot unit power settings, please see Appendix B: Connecting a Remote Reboot Unit.

User Administration

The User Administration options let you add and manage the users assigned to access the device.

NOTE: To perform functions on the Device Configuration menu, you must be logged in as *admin* or as a user with administrator rights.



To Add a User and Assign Rights

1. In the User ID field, enter the ID for your new user. They will be required to enter the User ID when logging in to the device. The User ID can be a maximum of 32 characters.
2. In the User Name field, enter the user name. This is a way to identify the user. The User Name can be a maximum of 32 characters.
3. In the Password and Confirm Password fields, enter a password for the new user. They will be required to enter this password when logging in to the device.
4. Choose the Rights access you want this user to have:
   - **Full Control of Remote Host**: These users can view and control the managed host computer. They can also power the remote host on and off if a remote reboot unit is used. See Appendix B: Connecting a Remote Reboot Unit.
   - **Administrator**: These users can view and control the managed host computer, as well as add/delete/edit other users' access rights.
5. Click the **Update** or **Add User** button to save the new information.

You can use the **Delete User** button to remove a user from your list. To edit a user's information, click on their name in the user's list, edit the information, and click the **Update** button.

Security

The security setting allows you to choose the level of security for your device and view your security log files. The security settings you select will affect the speed and performance of your device.

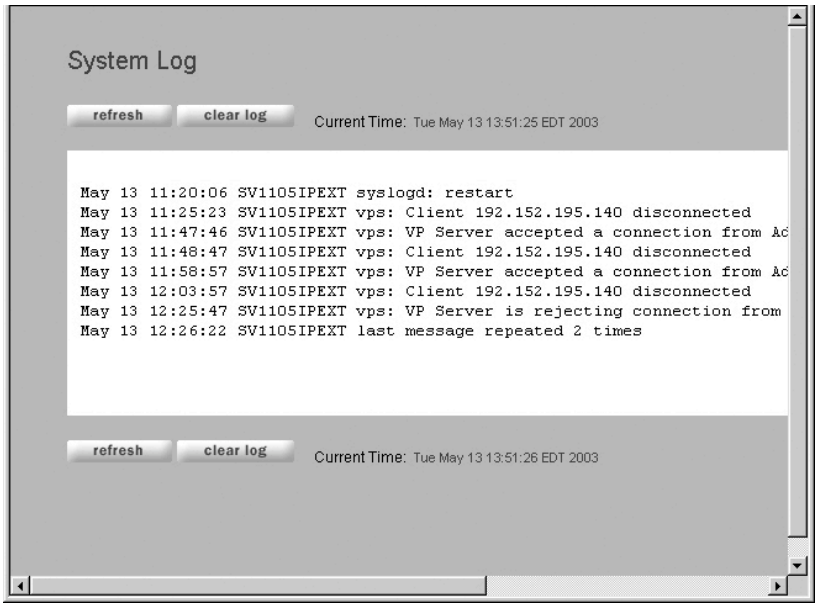
Level 0: At Level 0, there is no encryption. This will provide you with a standard level of security and will allow the device to work at its fastest speed.
Level 1: At Level 1, there is encryption of your keyboard and mouse data. This will provide you with a high level of security and still allow your device to run at a high speed.
Level 2: At Level 2, your keyboard, mouse, and video data is encrypted. This will provide the highest level of security, but will reduce the speed of your device.

When you have chosen a security level, click **Apply Settings**.

You can also choose to restrict access to the web server through an SSL-encrypted connection (e.g., https://…). When you select this option, you will be prompted to log in again under the secure address. To disable SSL-only connections, you will need to uncheck the "SSL connections only" box and set Remote Session Encryption back to Level O. You can also choose to allow Telnet and FTP connections. You will need to check this box if you want to use a Telnet Client to view debug information (See Appendix A: Viewing Debug Information).

View Logs

Clicking on the View Logs button allows you to view activities and events that have occurred on the managed host computer. You can view user login and remote session activity, administrative functions such as users or passwords being added or updated, launched remote control sessions, or changes made to device configuration settings.



NOTE: To view the logs, you must be logged in as *admin* or as a user with administration rights (see "User Administration on page 9 for details).

Refresh: Clicking the refresh button will update the System Log window with any activity that has occurred on the managed host computer since the log was opened or the last refresh was performed.

Clear Log: Clicking the clear log button flushes all log file data and starts a new log of activity occuring on the managed host computer. Log files start to over-write after 400kBytes of data is logged. You will be asked to confirm that you want to permanently delete all log data.

Printing, Saving, or Emailing the Log File: From your web browser, click on the **File** button. From the dropdown menu, you can choose to save, print, or send the log file.

Launching the Viewer

After setting the IP address and completing the initial setup process, you can launch the viewer to verify that the remote client can communicate with the managed host computer.

1. From the remote client Welcome page, click the **Launch Viewer** button located at the bottom right of the screen.
2. Accept the security certificate, if one if presented.
3. Enter the IP address of the device, if prompted.
4. From the viewer screen, you can now monitor the managed host computer, control its keyboard and mouse, and execute tasks on it.

There are four menus available from the Viewer screen: Shortcuts, Options, Connection, and About.

Shortcuts

The shortcuts menu provides quick access to the following common keystrokes and commands to help you manage and control your environment:

Ctrl-Alt-Del	Executes Ctrl-Alt-Del command
Start Menu	Enables access to Windows Start Menu programs and files
Task Manager	Enables access to Windows Task Manager
Close Window	Closes current window
Close MDI Window	Closes a multi document interface (MDI) frame or pop-up window
Scroll Lock x 2	Used with KVM switches
Next Window	Moves focus to one of the open windows
Print Screen	Copies current VP viewer screen data to copy buffer
Print Window	Copies current window to printer
Hold Down Ctrl Key	Used with KVM switches
Hold Down Alt Key	Used with KVM switches
Exit VP Viewer Client	Closes VP viewer and remote session

Options

The options dropdown menu provides access to the following additional settings to help you fine-tine your operating environment:

Force Screen Refresh	Refreshes screen to original quality.
Toggle Full Screen	Toggles screen size.
Viewer Options	This selection will open up a separate dialog box. From here, you can choose your quality vs. speed settings, set your horizontal/vertical screen alignment, or force the screen to auto-align if the video screen borders are not aligned within the Viewer.
Show frames/sec and network bits/sec	This selection shows the current bandwidth usage in frames per second and bits per second. The information is shown in the top bar of the viewer screen.

Connection

The connections dropdown menu enables you to manually set the compression and throttle line speed for optimum performance and security. Lower encryption levels can increase performance.

56K	Dialup speeds, lowest speeds, highest compression
DSL	Low speeds (500Kbps), high compression
T1	1 Mbits/sec, high compression
Low BW LAN	2 Mbits/sec, low bandwidth LAN speeds, medium compression
LAN	10 Mbits/sec, lowest compression
Auto	Performance algorithms select the best line speed limits and compression levels for optimum performance
Encrypt Everything	All data, video, keyboard, and mouse data is encrypted. This setting is normally done on the web server's security configuration page.
Encrypt KB & Mouse	Only keyboard and mouse data are encrypted. This setting is normally done on the web server's security configuration page.
No Encryption	No data is encrypted. This setting is normally done on the web server's security configuration page.
High Color	Uses slowest speed performance but best color performance
Low Color	Uses slow speed performance reduced color performance
Gray Scale	Uses higher speed performance but uses gray scale colors

Using the VPS Find Utility

The VPS find utility searches for other VP devices installed in a network segment.

1. Insert the VPS Find utility disk into your disk drive. Launch the **VPSFind.exe** file.
2. From the dialog box, type the network broadcast address of the segment you want to search and click **Find VP Servers**.
3. If you want to access and of the discovered VP Servers, you can highlight the desired device and click **Browse** to selected server.
4. When you are finished, click **Exit**.

Troubleshooting

If you are experiencing trouble with your device, first make sure that all cables are connected to their proper ports and are firmly seated. You may also want to try resetting the device by clicking on the **Reset Power** button. If problems persist, you can do a full reset by using a pen (or similar) to press the factory restore button located on the back of the device. Using the factory restore button will **delete all your configurations and restore the device back to the factory defaults**. You will have to go through the initial setup procedure again.

Video response is slow to respond or erratic.

- Verify that the managed host computer video configuration is set to a supported resolution and refresh rate. Optimum video resolution is 1024 x 768 @ 75Hz. For a list of supported video resolutions and refresh rates, see Video Settings on page 21.

Video displays pink screen.

- Verify that the managed host computer is turned on.
- Verify that the video refresh rate on the managed host is set to 85Hz or lower.
- Re-establish video communication using power-on reset.
- Reboot the managed host computer as needed.

Mouse pointer or mouse buttons slow to respond or erratic.

- Re-sync the mouse using the left-click or moving it across the screen several times (for at least five seconds).

Mouse pointer is out of sync with local mouse "dot."

- Verify that the managed host computer mouse acceleration is turned off. See "Mouse Acceleration" on page 3.

Can't communicate with the device after power-on reset or new installation.

- Wait 10 seconds after resetting before attempting to access the device.
- Ensure that the correct IP address has been entered in the browser.
- If you have performed a "factory default restore," the IP address has been reset to 192.168.1.254.
- If you are operating behind a firewall, make sure that all the appropriate ports have been opened. See "Accessing the Device Through a Firewall" on page 6.

Appendix A: Viewing System Configuration for the Device

There are three ways to view debug information. You can connect a serial console, or you can use a Telnet or FTP client.

Using a Debug Console

The steps below describe how to connect a serial console and use it with an RS-232 client to help monitor and configure the device.

1. Designate a client computer near the device to configure as a serial console.
2. Attach a serial RJ-12 cable to the Console port on the front of the device. Plug the other end into a COM port on the computer you have designated as the serial console.
3. From the serial console computer, launch HyperTerminal (available with all versions of Windows. Log in as user *root*) and configure a session to the following settings:
    - Connect Using: COM1 (or other COM port)
    - Port Speed: 115200
    - Flow Control: None
    - Data Bits: 8
    - Parity: None
    - Stop bits: 1

4. From the serial console client screen, you can login and view system configuration information.

Using a Telnet Client

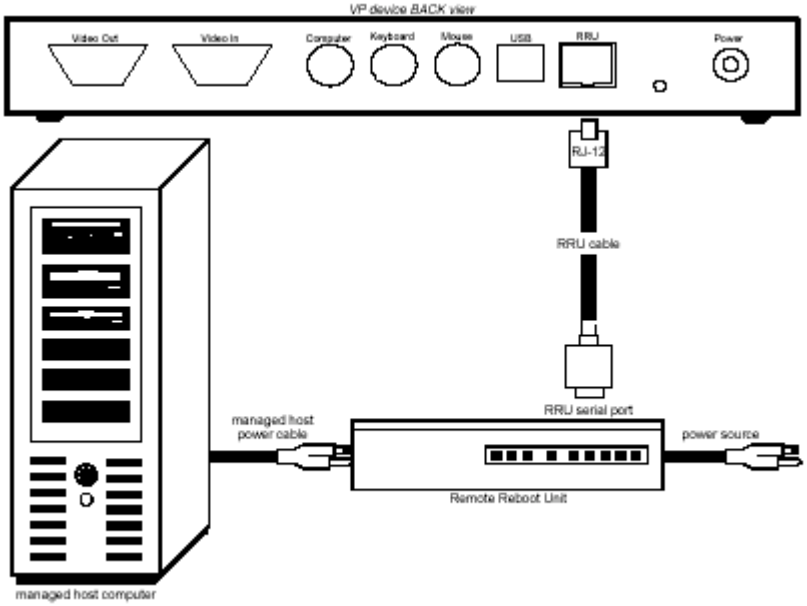
1. Configure a Telnet client session to use standard port 23 and TCP/IP connection.
2. Logon to the SV1105IPEXT as *admin* and make sure that you have checked the "Allow Telnet and FTP connections" box on the Security screen.
3. From the Telnet client, you can now access all NetBSD (UNIX OS) commands, including:
   `su root [no password]`

Using an FTP Client

1. Make sure that you have checked the "Allow Telnet and FTP connections" box on the Security screen.
2. From a DOS prompt or FTP client, type the following command:
   `ftp <device IP address>`
3. From the FTP prompt, login to the VP device as *admin*. You can now access the standard FTP commands and execute them on the VP device.

Appendix B: Connecting a Remote Reboot Unit

1. Connect your device to your managed host computer as described in the Installation section on page 4.
2. Using a serial to RJ-12 cable, connect the RRU port on the device to a serial port on the remote reboot unit.
3. Attach the managed host computer's power cable to the remote reboot unit's power port.
4. Connect the remote reboot unit's power cable to a grounded power source.



Configuring remote reboot unit power settings

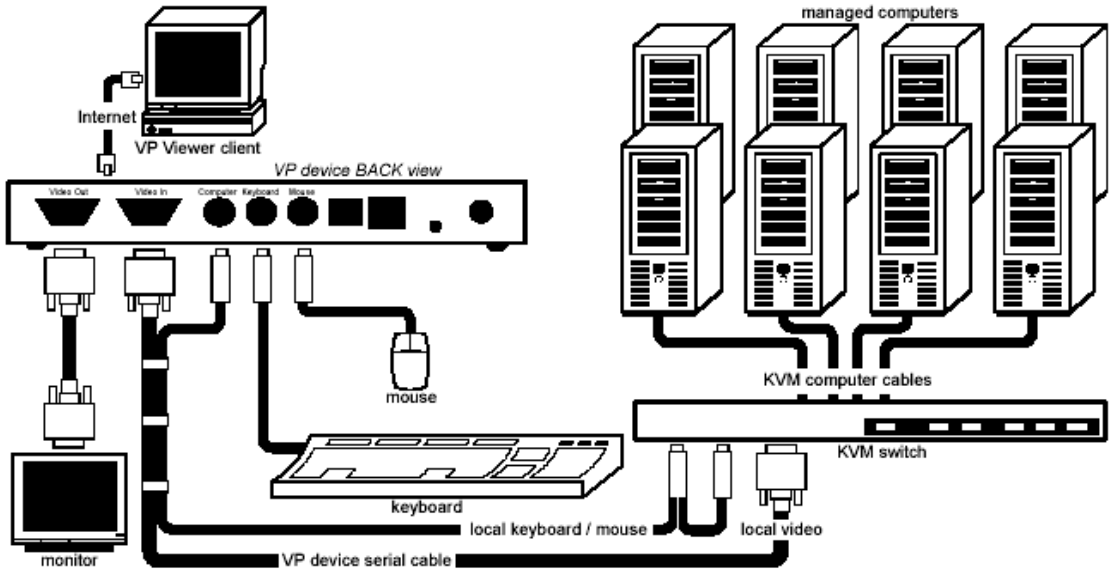
NOTE: To configure the remote reboot unit power settings, you must be logged in as *admin* or as a user with administrator rights.

1. From the Device Configuration tab, click **Configure Power**.
2. In the Description field, type the name of the remote reboot unit.
3. In the Power ON, Power OFF and Toggle Power fields, type the sequence strings you want to apply to each operation and click Apply Settings.
4. The Power Control tabs at the bottom of the web server pages will act according to the remote reboot unit settings. (The "Reset Power" tab uses the "Toggle Power" sequence settings)

Appendix C: Alternative Configurations

Connecting a KVM switch

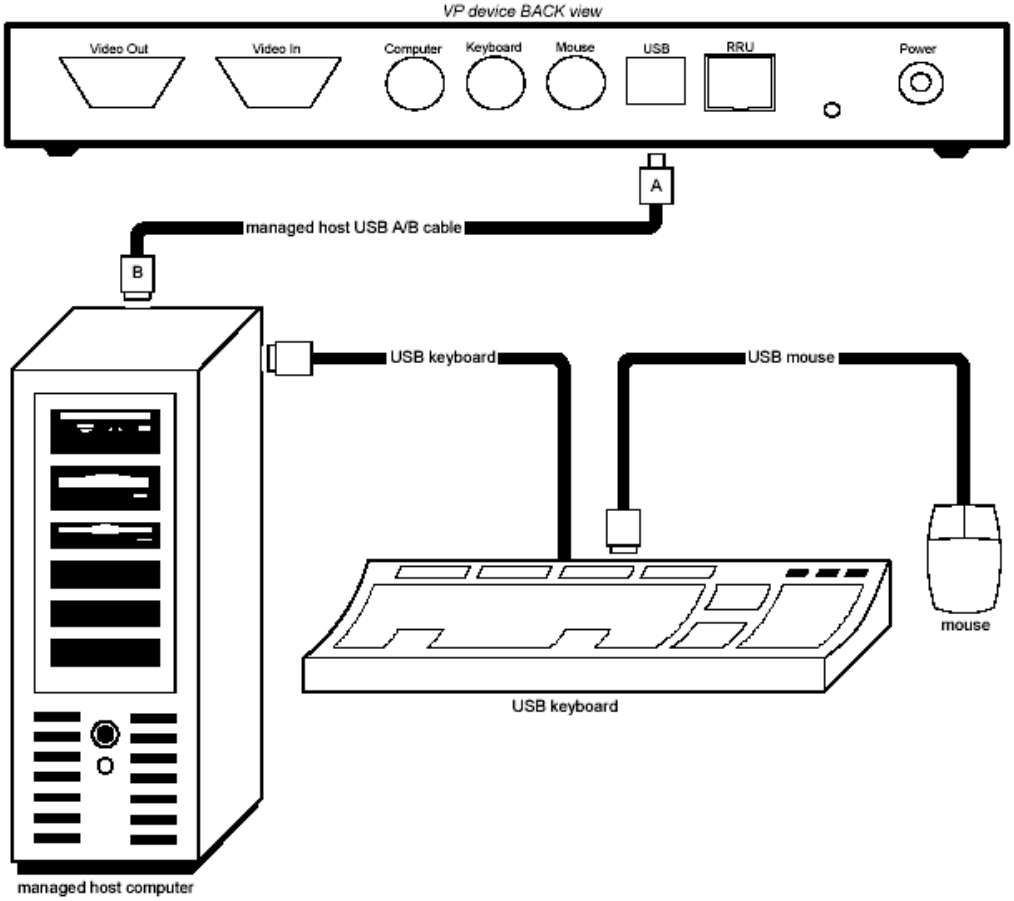
You can configure the device with a KVM switch to enable you to pass the KVM output to the Internet. Using a client computer, you can control managed computers connected to the KVM switch.



1. Attach the managed computers to a KVM switch as outlined in the KVM manufacturer documentation and set the KVM switch to pass output to the managed computer you want to control.
2. Attach the cable female video connector (black) to the Video In port on the back of the VP device and attach the cable male video connector (blue) to the KVM switch local video port.
3. Attach the cable computer connector (black) to the device's Computer port.
4. Attach the cable keyboard connector (purple) and mouse connector (green) to the KVM switch local keyboard and mouse ports.
5. Attach a keyboard and mouse directly to the device's Keyboard and Mouse ports.
6. Attach a monitor by connecting the monitor video cable to the VP device Video Out port.
7. Attach the device to your network using the Network port on the front of the VP device.
8. From a client web browser, type the device address, log in to the Web Server, and launch the Viewer to access the managed computer configured to receive KVM input.

Appendix D: Using a USB Keyboard and Mouse

The steps below describe how to connect a USB keyboard and mouse to the device.



1. Using a USB A/B cable (not included), plug the “A” end of the cable into the device’s USB port.
2. Plug “B” end of the cable into a USB port on the managed host computer.
3. Plug the USB keyboard and mouse into the two other USB ports on the managed host computer.

Appendix E: Replacing the Default Server Certificate

You can replace the default VP device server certificate with a different one. Make sure the new certificate is in PEM format and at least 1025 bits in size.

1. Open an FTP session and log in to the VP device as user *admin*.
2. Replace the default server certification with a new certificate by typing the following FTP command:

```
put <new_certificate.pem>
      /flash/inc/server.pem
```

3. Cycle power to the VP device. The new service certificate is now in place.

Technical Specifications

Hardware Specifications

Embedded System:

- 32-bit embedded processor
- 40 Meg SDRAM
- 8 Meg flash memory
- Real Time Clock
- Onboard 10/100 Ethernet NIC

Video:

- VGA compatible
- 1280x1024 @ 60 Hz max
- Video in, standard VGA connection (DB-15)
- Video out, standard VGA connection (DB-15)

Keyboard & Mouse:

- Host Keyboard and Mouse cable to Computer connection (Mini DIN 8)
- Real Keyboard standard PS/2 connection (Mini DIN 6)
- Real Mouse connection standard PS/2 (Mini DIN 6)

Communications channels:

- Ethernet port:
  - 10/100 mbps Ethernet
  - RJ-45 connection

- Serial Debug port (RJ12 connector):
  Used for embedded system configuration and control
  Settings:
  - 115200 bps
  - Flow control: None
  - Data bits: 8
  - Stop bits: 1
  - No Parity

- USB port:
  - USB-B series connector
  - USB v. 1.1

- RRU port:
  Serial port designated to control external remote reboot units
  Settings:
  - 9600 bps
  - Flow control: None
  - Data bits: 8
  - Stop bits: 1
  - No parity

Configuration:

- Factory default restore pushbutton switch next to power supply jack
  - Hold in for one second and release to reset VP device to original factory settings.
  - User and device configuration data is not preserved

Electrical:

- Power supply
  - External +12v DC @ 500 mA
  - Connector polarity:
    External ring negative
    Internal ring +12v DC
    Power Consumption: 3W

Mechanical:

- Enclosure: 1 x 4.5 x 7.75 in. (25.4 x 114.3 x 196.9 mm)

Software specifications

- NetBSD 1.6 Operating System
- Onboard web server
- Custom Virtual Presence client launches from the VP device web server
- Custom onboard Virtual Presence server
- No drivers or any other software configuration required
- Security:
  - 128 bit SSL v2, v3 and TLS v1 web encryption
  - RC4 algorithm for the data stream
  - MD5-secured password
  - Unlimited user accounts

Video Settings

512 x 384	70Hz
720 x 400	60Hz, 70Hz, 75Hz, 85Hz, 100Hz
640 x 480	60Hz, 67Hz, 72Hz, 75Hz, 85Hz, 90Hz, 100Hz, 120Hz, 140Hz
800 x 600	56Hz, 60Hz, 72Hz, 75Hz, 85Hz, 90Hz, 100Hz, 120Hz, 140Hz
832 x 624	75Hz
960 x 720	60Hz, 75Hz, 85Hz
1024 x 768	60Hz, 70Hz, 75Hz, 80Hz, 85Hz, 90Hz, 100Hz
1024 x 800	60Hz
1152 x 864	60Hz, 70Hz, 75Hz, 76Hz, 80Hz, 85Hz
1152 x 900	67Hz
1280 x 960	60Hz, 75Hz, 85Hz
1280 x 1024	60Hz, 67Hz, 75Hz, 85Hz

Technical Support

The following technical resources are available for this StarTech.com product:
On-line help:
We are constantly adding new information to the *Tech Support* section of our web site. To access this page, click the *Tech Support* link on our homepage, **www.startech.com**. In the tech support section there are a number of options that can provide assistance with this card.

Knowledge Base - This tool allows you to search for answers to common issues using key words that describe the product and your issue.

FAQ - This tool provides quick answers to the top questions asked by our customers.

Downloads - This selection takes you to our driver download page where you can find the latest drivers for this product.

Call StarTech.com tech support for help: **1-519-455-4931**
Support hours: Monday to Friday 9:00AM to 5:00PM EST (except holidays)

Warranty Information

This product is backed by a one-year warranty. In addition StarTech.com warrants its products against defects in materials and workmanship for the periods noted below, following the initial date of purchase. During this period, the products may be returned for repair, or replacement with equivalent products at our discretion. The warranty covers parts and labor costs only. StarTech.com does not warrant its products from defects or damages arising from misuse, abuse, alteration, or normal wear and tear.

Limitation of Liability
In no event shall the liability to StarTech.com Ltd. (or its officers, directors, employees or agents) for any damages (whether direct or indirect, special, punitive incidental, consequential, or otherwise), loss of profits, loss of business, or any pecuniary loss, arising out of related to the use of the product exceed the actual price paid for the product. Some states do not allow the exclusion or limitation of incidental or consequential damages. If such laws apply, the limitations or exclusions contained in this statement may not apply to you.

NOTE: The associated software contains encryption technology subject to the U.S. Export Administration Regulations and other U.S. law, and may not be exported or re-exported to certain countries or to persons or entities prohibited from receiving U.S. exports (including Denied Parties, entities on the Bureau of Export Administration Entity List, and Specially Designated Nationals). For more information on the U.S. Export Administration Regulations (EAR), 15 C.F.R. Parts 730-774, and the Bureau of Export Administration (BXA), see the BXA homepage at http://www.bxa.doc.gov

FCC Compliance

This device complies with part 15 of the FCC Rules and also with European standards EN55022. Operation is subject to the following conditions: (1) this device may not cause harmful interference; and (2) this device must accept any interference received, including interference that may cause undesired operation.

May 30, 2003